

Risk Management



EHR DOCUMENTATION: How to Keep Your Patients Safe, Keep Your Hard-Earned Money, and Stay Out of Court

by Donna Vanderpool, MBA, JD

Innov Clin Neurosci. 2015;12(7-8):34-38

This ongoing column is dedicated to providing information to our readers on managing legal risks associated with medical practice. We invite questions from our readers. The answers are provided by PRMS, Inc. (www.prms.com), a manager of medical professional liability insurance programs with services that include risk management consultation, education and onsite risk management audits, and other resources to healthcare providers to help improve patient outcomes and reduce professional liability risk. The answers published in this column represent those of only one risk management consulting company. Other risk management consulting companies or insurance carriers may provide different advice, and readers should take this into consideration. The information in this column does not constitute legal advice. For legal advice, contact your personal attorney. Note: The information and recommendations in this article are applicable to physicians and other healthcare professionals so “clinician” is used to indicate all treatment team members.

QUESTION

“I am considering implementing a new EHR system. According to the vendor’s marketing material and the salesperson, the EHR system will increase my revenue by automatically increasing the documentation required to support the higher level E/M codes. Is this too good to actually be true?”

ANSWER

You are right to be concerned. You should focus on creating accurate documentation rather than creating documentation that supports higher level coding for services that are not medically necessary. The goal should be to document your decision-making so your work can be understood by others, such as subsequent treaters, or even expert witnesses supporting or questioning your care in litigation years later.

RISK MANAGEMENT STRATEGY #1: DOCUMENT WHAT YOU DID AND WHY, AS WELL AS WHAT YOU CONSIDERED BUT REJECTED AND WHY

Say you have a patient with suicidal ideation—you document that you think he should be hospitalized and that voluntary hospitalization was offered to him, but he declined. You also document that you considered involuntary hospitalization, but the patient didn’t meet the criteria. Further, you document that you adjusted the treatment plan—maybe changing medications, increasing the frequency of visits, requiring the patient to check in by phone, and discussing your concerns with the patient’s significant other. You explain in your documentation what you did and why. The Florida Board of Medicine is one example of a licensing board that has put this expectation into a regulation that states “A licensed physician shall

maintain patient medical records... with sufficient detail to clearly demonstrate why the course of treatment was undertaken.”¹

When considering documentation for billing purposes, physicians should be aware of the significance of electronic health records (EHRs), specifically the increased regulatory risks related to coding and data protection, the risks to patient safety, and last, but not least, the risks related to malpractice.

HOW TO KEEP YOUR HARD-EARNED MONEY

The first regulatory risk of documentation in EHRs is coding risk. The Federal False Claims Act (FCA) protects the federal government from being overcharged or sold substandard goods or services. The FCA imposes civil liability on any person who knowingly submits, or causes to be submitted, a false or fraudulent claim to the federal government. The “knowing” standard includes acting in deliberate ignorance or reckless disregard of the truth or falsity of the information related to the claim. An example is a provider who knowingly submits claims for services not provided. Civil penalties for violating the FCA may include fines up to three times the amount of damages sustained by the government as a result of the false claims, plus \$11,000 per claim filed. FCA criminal penalties for submitting false claims may include fines, imprisonment, or both. When the federal government pays for items or services rendered to Medicare beneficiaries, the federal fraud and abuse laws apply. Many similar state laws apply to services under state-financed programs and under private-pay insurers.

What is the relevance of fraud and abuse? Any bill you submit to

the federal government includes your certification that the payment requested was earned and that you complied with the billing requirements. There are many examples of improper claims submitted to the federal government, including billing for services that were not medically necessary. For example, a completed and documented complex review of systems that was medically unnecessary (e.g., on your psychotherapy patient that is seen weekly) cannot be billed at the highest code because the services provided with the full exam were not medically necessary.

In 2012, an article appeared in the *New York Times*² noting that the federal government is spending billions of dollars in incentives to push hospitals and doctors to use electronic records. However, the move to EHRs may be contributing to billions of dollars in higher costs for Medicare, private insurers, and patients by making it easier for providers to bill more for their services, whether or not they provide additional care. In the article, one doctor expressed concern with a new EHR and said the new system prompted doctors to click a box that indicated a thorough review of patients’ symptoms had taken place, even though the exams were rarely performed. Another function let doctors pull exam findings “from thin air” and include them in patients’ records. And the article notes, as software vendors race to sell their systems, many are straightforward in extolling the benefits of those systems in helping doctors increase their revenue. One vendor promises that it “plays the level of service game on your behalf and beats them at their own game using their own rules.”

RISK MANAGEMENT STRATEGY #2: UNDERSTAND THAT JUST BECAUSE THE EHR CAN CREATE DOCUMENTATION SUPPORTING THE HIGHEST BILLING CODE DOES NOT MEAN IT IS APPROPRIATE TO BILL THE HIGHEST CODE

Medical necessity determines accurate coding, even if a coding tool suggests billing for a higher level of service. Immediately following the *New York Times* article, a letter³ was sent to hospitals from the Department of Health and Human Services (HHS) and the Department of Justice warning Medicare and Medicaid providers that EHRs are not to be used to “game the system” by having the system create extensive documentation and then upcoding. According to the letter, progress notes created with limited space EHR templates are not sufficient documentation. The government also indicated its dislike of check boxes, drop down menus, limited space to enter data, or pre-defined answers. From the letter:

“False documentation of care is not just bad care; it’s illegal. These indications [of fraud] include potential ‘cloning’ of medical records in order to inflate what providers get paid. There are also reports that some hospitals may be using EHRs to facilitate upcoding of the intensity of care or severity of patients’ conditions as a means to profit with no commensurate improvement in the quality of care...A patient’s care information must be verified individually to ensure accuracy: it cannot be cut and pasted from a different record of the patient, which risks medical errors as well as overpayments.”

Then in 2013, the HHS Inspector General issued a report⁴ indicating providers have failed to implement fraud protection safeguards in EHR technology. The report included two

EHR documentation practices that could be used to commit fraud, the first being copy and paste, and the second was over-documenting irrelevant documentation just to support higher level billing via auto-populating fields and checkboxes. The resulting documentation can suggest that the provider provided more comprehensive services than were actually rendered. Last year HHS's Office of Inspector General (OIG) issued another report⁵ saying not enough is being done to address these EHR billing issues, and the OIG is not giving up on this. This year's report⁶ of unimplemented recommendations points out that CMS does not have a plan to detect and reduce fraud in EHRs with respect to billing for services.

The Federation of State Medical Boards (FSMB) has also expressed concerns about copy and paste. In a FSMB report,⁷ the following is included in the section on ethical utilization of EHRs: "Generally it is inappropriate to copy and paste or otherwise document an entry that is not derived from a patient encounter at the time of the visit, unless the provider makes a clear notation that the information is copied and pasted from another record."

Other ways to automate documentation include the following:

Templates. Be cautious of templates with pre-printed information indicating the highest level of services was performed. Also, make sure the template is appropriate; templates tend to take a one-size-fits-all approach, without regard for age appropriateness, or target patient population.

Pre-populating fields. Some EHRs can populate an entire patient assessment just by selecting a check box, such as populating an entire review of systems. In one case, the prepopulated data for physical

examinations created automated documentation saying the female patients had received prostate exams and male patients had negative pap smears! Again, some state boards⁸ have formally expressed specific concerns about the pre-population feature in EHRs. The North Carolina Board cautions against relying upon software that pre-populates particular fields in the EMR without updating those fields in order to create a medical record that accurately reflects the elements delineated in a position statement.

Default data. Be sure you know what is documented (that is, what shows up in the record) if you do not enter data in a field.

Documenting by exception. Some EHRs offer the ability to mark a single checkbox indicating that all patient systems are either normal or abnormal. When the doctor mistakenly checks the wrong box, the documentation is all wrong.

Remember that documentation created by an EHR is not the same as documentation created by the healthcare provider. Consequently, it is a problem if a reader cannot distinguish between data entered by the provider and system-generated data. Documentation must be specific to the patient, and to the patient's visit. Free text space should be available to individualize the services provided.

With all of this electronic documentation comes data protection risks. There are many reports⁹ of government investigations of breaches of protected health information, particularly unencrypted laptops with patient information being stolen. These major enforcement actions underscore the significant risk to the security of patient information posed by unencrypted laptop computers and other mobile devices. And it's not just

Health Insurance Portability and Accountability Act of 1996 (HIPAA) enforcement to worry about. States can also regulate consumer data protection and require the protection of personal information.

HOW TO KEEP YOUR PATIENTS SAFE

Risk managers have been concerned about EHRs and patient safety for years. Now it's getting a lot of attention. The Joint Commission recently issued a Sentinel Event Alert¹⁰ on the safe use of health information technology, and gave several examples of adverse events caused by EHRs. Also, the ECRI Institute put out its Top 10 Patient Safety Concerns for 2015.¹¹ Second on the list of concerns was data integrity (e.g., incorrect or missing data in EHRs, including one patient's data in another patient's record, missing data or delayed data delivery, default values being used by mistake, or fields being prepopulated with erroneous data, and outdated information being copied and pasted into a new report). Tenth on the list was medication errors related to pounds and kilograms. Although the problem poses a significant potential for error with adults, children and older adults may be even more sensitive to medication dosing errors. Here are some additional patient safety problems that have been attributed to the use of EHRs:

Box checking. Important information can be omitted if you only check the boxes.

Drop boxes. These can be very sensitive in terms of making a choice; clicking just a millimeter off changes the entry. This is of particular concern in lawsuits involving psychopharmacology, where the prescriber clicked on (ordered) a different amount than intended just because the cursor was a millimeter off.

Information overload. EHRs can create too much information. There can be so much information that providers cannot find the pertinent information, or pertinent data could be overlooked.

Amending data. This can be difficult. Also, given the fluid nature of an EHR, amending data can be misleading. In one case, the patient entered the hospital and indicated she had no known drug allergies. She was prescribed a medication for the first time and had an allergic reaction. The EHR was updated to list the allergy, but it updated it everywhere in the record, including in the admission notes. So it appeared as if she came into the hospital allergic to the medication that was prescribed, making the prescriber appear negligent.

Templates. Templates create notes that look the same as every other note and may not create a record that is accurate for the patient and for the patient encounter. For example, there have been reports of adult templates used to document exams of children.

Decision-support tools. Be aware that many EHR users complain that tools, such as safety alerts and clinical treatment algorithms, are not applicable to their treatment. To go through many inapplicable safety alerts leads to alert fatigue, which can result in a relevant safety alert being overridden without review. Lack of appropriate clinical algorithms became an important fact in one medical malpractice case¹² where the patient presented to the emergency department with complaints of severe calf pain and swelling. He was discharged with a diagnosis of viral gastroenteritis. Less than two days later, the patient died at a different hospital of necrotizing fasciitis. The court, in its opinion, placed the liability issue on the

templates and decision support tools in the hospital's EHR and said:

"The EMR templates are directed towards the chief complaint [which the doctor chooses] that also pertains to everything, your assessment and plan at the end of the chart. Here the chief complaint chosen by Dr. Kwon was fever, even though she acknowledges that Mr. Bowman did not have a fever at the time. She indicated that she had no option regarding the use of a template: you have to choose a template, and by that choice, a screen pops up and provides the doctor with other options or choices to make. So for example, there are different templates for other chief complaints, which include, as examples, ones for chest pain or abdominal pain. Further, the chosen templates have prompts as to certain medical information to be filled in... The resident who saw the patient in the emergency department said in a deposition that she was bound by the diagnostic system's templates for complaints that guide doctors' assessments and treatment plans."

HOW TO STAY OUT OF COURT

The case above illustrates that a provider's use of EHRs can lead to allegations of professional liability. The critical role of expert witnesses in malpractice litigation makes adequate documentation necessary. The expert will base his opinion, in part, on the record. The documented record stands as a testament of treatment provided and the reasoning behind it. Your documentation is your defense. Defensible cases where the provider delivered seemingly excellent care have been lost or settled because of poor documentation. Without documentation that supports the care that was given, it is difficult or

impossible to find a supportive expert witness to help defend a case, thereby making it easier for plaintiff to prevail. The most powerful thing you can do in terms of having a defense in the event of a claim, lawsuit, or administrative action is to document the basis for your clinical decision making.

In litigation, physicians' professional judgment carries a lot of weight. Courts will defer to the treating physician—as long as there is something to base that deference on, and that is your contemporaneous documentation. There is more than one way to treat a patient. Physicians use their clinical judgment in making treatment decisions. A physician can use proper clinical judgment and there may still be a bad outcome, such as a bad reaction to a medication. The bad outcome may not be a result of malpractice, but if a lawsuit ensues—what do we want to know? Why did the physician do what she did? How do we know that? We should know it from the record. Also, do not give a plaintiff's expert witness the opportunity to make up his or her own theory of why you made a particular treatment decision. State it in the record. Liability issues with EHRs include the following:

Templates. Templates can cause all documentation to look the same. That can lead to credibility problems in the courtroom.

Metadata. The computer keeps track of everything that is done, and how long it took to do it. Think about the problem of alert fatigue, i.e., there are so many irrelevant alerts that users just override all of them. In a particular case, if all alerts are just automatically overridden, and there is an adverse event, and that event could be tied to an alert, the computer will show exactly how long it took for the provider to override that alert. If the provider had alert

fatigue and did not even review the alert, that time will be very, very short. The plaintiff's attorney will get that data in discovery, and will use that time to argue the provider did not even care enough to review relevant alerts.

Information overload. It can be very difficult to find the clinically relevant information buried in all of the information in the EHR.

Overreliance on what others have put in the record. Providers need to do their own clinical assessment and not only rely on and use what others have entered into the record.

Input errors. Such errors are very easy with drop down boxes, default data, and pre-populated fields.

So be very careful when documenting. Check what your documentation actually says, and review the entry before finalizing it.

RISK MANAGEMENT STRATEGY #3: ADDRESS THE USE OF SHORTCUTS IN THE EHR.

Be careful with templates. Do not allow copy and paste, or if you do allow it, require author identification. Do not allow prepopulated or auto-populated fields. Add space for free-form text and encourage the use of free-form text to individualize the record entry. Consider periodically printing out a record to see the completeness and consider whether another provider could understand what you did and why just from your documentation.

REFERENCES

1. FAC § 64B8-9.003. Standards for Adequacy of Medical Records.
2. Abelson R, Creswell J, Palmer G. Medicare bills rise as records turn electronic. New York Times. September 21, 2012.
3. Letter from Obama Administration on hospital billing. New York Times. September 24, 2012. <http://www.nytimes.com/interactive/2012/09/25/business/25medicare-doc.html>.
4. US Dept. of Health and Human Services Office of Inspector General. Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology. December 9, 2013. oig.hhs.gov/oei/reports/oei-01-11-00570.asp.
5. US Dept. of Health and Human Services Office of Inspector General. CMS and Its Contractors Have Adopted Few Program Integrity Practices to Address Vulnerabilities in EHRs. January 2014. oig.hhs.gov/oei/reports/oei-01-11-00571.pdf.
6. US Dept. of Health and Human Services Office of Inspector General. Compendium of Unimplemented Recommendations. March 2015. oig.hhs.gov/reports-and-publications/compendium.
7. Federation of State Medical Boards. Report on the Committee on Ethics and Professionalism – Framework on Professionalism in the Adoption and Uses of Electronic Health Records. April 2014. www.fsmb.org/Media/Default/PDF/FSMB/Advocacy/ehr_framework_final_adopted.pdf.
8. North Carolina Medical Board. Position Statement on Medical Record Documentation. http://www.ncmedboard.org/resources-information/professional-resources/laws-rules-position-statements/position-statements/medical_record_documentation.
9. US Dept. of Health and Human Services. Case Examples and Resolution Agreements. www.hhs.gov/ocr/privacy/hipaa/enforcement/exempl.es/index.html.
10. Joint Commission. Safe use of health information technology. Sentinel Event Alert. 2005;54:1. www.jointcommission.org/assets/1/18/SEA_54.pdf.
11. ECRI Institute. Top 10 Patient Safety Concerns for Healthcare Organizations 2015. <https://www.ecri.org/Pages/Top-10-Patient-Safety-Concerns.aspx>.
12. Bowman v. St. Luke's Roosevelt Hosp. Ctr., 2011 NY Slip Op 32738(U) (Sup. Ct.).

AUTHOR AFFILIATION: Ms. Vanderpool is Vice President, Professional Risk Management Services, Inc. Arlington, Virginia.

ADDRESS FOR CORRESPONDENCE:

Donna Vanderpool, MBA, JD, Vice President, Professional Risk Management Services, Inc., 1401 Wilson Blvd., Suite 700, Arlington, VA 22209; E-mail: vanderpool@prms.com

SUBMIT YOUR OWN QUESTION

To submit a question, e-mail Elizabeth Klumpp, Executive Editor, eklumpp@matrixmedcom.com. Include "Risk Management Column" in the subject line of your e-mail. All chosen questions will be published anonymously. All questions are reviewed by the editors and are selected based upon interest, timeliness, and pertinence, as determined by the editors. There is no guarantee a submitted question will be published or answered. Questions that are not intended for publication by the authors should state this in the e-mail. Published questions are edited and may be shortened. ■